REMARKS

Claims 1-19 are currently pending in the application. Claims 1-7 and 10-17 are rejected under 35 U.S.C. § 102(b) as anticipated by Maes et al., U.S. Patent No.6,016,476. Claims 8-9 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Maes et al., in view of Lambert, et al., U.S. Patent No. 6,282,649. Claims 1-3 and 11 are further provisionally rejected under the doctrine of obviousness-type double patenting as being unpatentable over claims 1-3, and 9 of copending Application No. 10/132438.

Applicants respectfully traverse the rejections, but offer amendments to claims 1-3, 9-13, 16 and 19 to more clearly claim their invention.

As an overview, although Maes et al. discloses devices and processes that involve authentication steps, some of which are performed over a network, it is primarily directed at the provision of a "Universal Card" on which credit/debit card information is written for each transaction by a dedicated Personal Digital Assistant ("PDA") which stores encrypted card data that is accessed upon authentication at the PDA by use of biometrics or PIN/password on the condition of a valid (unexpired) digital certificate. Thus,

> the user *must* periodically connect the PDA device 10 with the central server 60 of the service provider (Link L1, FIG. 3) in order to obtain a valid digital certificate from the central server 60 prior to initiating a consumer transaction,

(Col. 7, lines 38-41 [emphasis added].)

> If the digital certificate is valid (i.e., unexpired) the requested card information is then retrieved from memory 14 and stored in the encrypter/decrypter module 24. The selected card information is then decrypted by the encryption/decryption module 24 using *an encryption key unique to the PDA device* 10 (step 214). The decrypted card information is then sent to the smartcard reader/writer 30 where it is then written to the Universal Card 26 (step 216). The Universal Card 26 is then removed from the smartcard reader/writer 30 and swept through the magnetic reading device of the transaction terminal 80 (FIG. 3) (step 218). The consumer transaction information is then sent to the proper financial institution 70 via communication link L4 (step 220).

(Col. 11, lines 27-40 [emphasis added]). In another embodiment cited by the Examiner, a system using just a "Smartcard" rather than the dedicated PDA is partially disclosed:

It is to be appreciated by one of ordinary skill in the art that a *special* ATM, kiosk or POS terminal can be employed to perform the methods and functions of the present invention in lieu of the actual PDA device, thereby eliminating the need to physically posses the PDA device 10. For instance, *a smartcard having a valid digital certificate and the user's verification data* (e.g, biometric data (voice print), PIN and/or password) and card information stored thereon may be inserted into the ATM, kiosk or POS terminal, which are be equipped with biometric sensors such as a microphone. *The ATM can then verify the user biometrically or via PIN or password.* Assuming the digital certificate is valid, the ATM can then initialize the smartcard which may then be used to perform, for example, a purchase transaction. The smartcard may then be used for the duration of the validity of the digital certificate (i.e., until the digital certificate expires) or until another card is loaded. In this embodiment, the smartcard can be used for only a limited amount of transactions. The digital certificate may be downloaded to the smartcard by any method analogous to the PIN maintenance techniques disclosed in the above incorporated U.S. Ser. No. 08/873,079, "Portable Acoustic Interface For Remote Access to Automatic Speech/Speaker Recognition Server." For example, the user may establish a communication link with the central server 60 service provider through a personal computer having a smartcard reader, whereby a valid *digital certificate* may be *download*[ed] onto the smartcard after the user provides verification information such as user ID, PIN, smartcard serial number, and/or biometric data.

(Col. 14, lines 27-46 [emphasis added].) Again, the authentication-for-access to card information is performed at the transaction location using only local information; a digital certificate is downloaded from the service provider upon a separate authentication at a different time. Although it is not stated explicitly, by reference to "the methods and functions of the present invention," the user's verification data is encrypted on the smartcard, but there is no mechanism for providing the decryption key.

In contrast to the dedicated device (and not clearly practical) scheme disclosed in Maes et al., the instant invention is addressed to authentication rather than access, avoids the use of "[encryption] keys typically kept . . . on a desktop or mobile computer" (para. 5) and "is usable with ordinary computers" (para. 7), "which, without limitation, may be a desktop or notebook computer at home, at work or at a point-of-sale-or-service kiosk)" (para. 12). In the embodiments shown in Figs. 1 and 2, authentication is performed at the time of the transaction by matching user identification information, not at the user device or the authentication-seeking entity, but at the trusted third party (authentication server), with encrypted card-resident information communicated to the authentication server through the authentication-seeking entity in both cases and the user password communicated to the authentication server through the

authentication-seeking entity in Fig. 1 and directly in Fig. 2. To more clearly emphasize this inventive approach, claims 1 and 11 are amended to use the "ordinary computer" language from the specification, to more specifically state the storage media is read by "any ordinary computer" (capable of reading the media and connecting to the network), not a dedicated or special device with stored authentication information as disclosed in Maes et al., and that the remote authentication server receives and matches the authentication information at the time of the transaction based on the personal code. Claims 2, 3, 10, 12 and 13 are amended to conform to the "ordinary computer" language. Claims 6 and 16 are amended to correct the antecedent reference to "personal code" from "personal information". Claims 9 and 19 are amended to correct the antecedent to "transaction party" from "user".

Applicants respectfully submit that, as amended, the claims clearly distinguish over Maes et al. and Maes et al. in view of Lambert et al.

35 U.S.C. § 102(b) Rejections

Maes et al. does not anticipate any of claims 1-7 and 10-17 as it fails to disclose the claimed systems, computer program module and processes with all the limitations of claim, among others, notably the reading of the storage medium by "any ordinary computer" and transmission of read information *to* a remote authentication server for matching based on a personal code.

Responding specifically to paragraph 3 of the Office Action, Maes et al. at col. 7, lines 57-65, does not disclose a system for authentication of a party in a transaction conducted over a communication network; those lines disclose authentication for downloading a digital certificate; the underlying transaction is conducted at a point-of-sale card-swipe-reader or kiosk. The smartcard disclosed at Maes et al. at col. 14, lines 21-22, is not read by an "ordinary computer", but "a special ATM, kiosk or POS terminal." Maes et al. does not disclose receipt by a remote authentication server of the information stored on the storage media to be matched at the server based on the personal code; col. 8, lines 25-27 cited by the Examiner discloses the prompting for and impliedly receipt of a PIN for the transmission, not receipt, of a digital certificate (lines 28-

31). Col. 14, lines 17-46, also cited by the Examiner, refers to also to the transmission of a digital certificate, not receipt of stored information for matching to a data base. Maes et al. does not disclose a wallet-sized storage medium read by an ordinary computer as part of a transaction or an authentication server that receives the read information and a personal code at the time of the transaction. It should be clear from context that the "transaction" of the claim is not the authentication process itself; but even if the authentication process were considered a "transaction", Maes et al. does not disclose the receipt and matching by an authentication server of information read from the storage medium by an ordinary computer. Claim 1 is not anticipated by Maes et al.

Responding to paragraph 4 of the Office Action regarding claim 2, Maes et al. at col. 14, lines 17-45, does not disclose claim 2's transmission from an "ordinary computer" through a second computer; it discloses the creation of a "special" ATM, kiosk or POS terminal "in lieu of the actual PDA device" (lines 17-21) that reads the smartcard. In that embodiment, there is no first computer as required expressly by claim 2 and claim 1 from which it depends. Claim 2 is no way anticipated by Maes et al.

Similarly, responding to paragraph 5 of the Office Action regarding claim 3, Maes et al. at col. 14, lines 21-26, does not disclose claim 3's transmission from an "ordinary computer" through a second computer; it discloses the creation of a "special" ATM, kiosk or POS terminal "in lieu of the actual PDA device" (lines 17-21) that reads the smartcard. Again, in that embodiment, there is no first computer as required expressly by claim 3 and claim 1 from which it depends. Claim 3 is no way anticipated by Maes et al.

Responding to paragraph 6 of the Office Action regarding claim 4, Maes et al. does not disclose one-use tokens that are read by an "ordinary computer" and received by a remote authentication server for matching based on a personal code as required by claim 1 as limited by claim 4. Claim 4 is in no way anticipated by Maes et al.

Responding to paragraph 7 of the Office Action regarding claim 5, Maes et al. at col. 14, lines 21-24 does not disclose claim a digital certificate that is read by an "ordinary computer" and received by a remote authentication server for matching based on a personal code as required by claim 1 as limited by claim 5. The digital certificate disclosed in Maes et al. is checked for validity (expiration) at either the special PDA or the special ATM, kiosk or POS terminal. Claim 5 is not anticipated by Maes et al.

Responding to paragraph 8 of the Office Action regarding claim 6, Maes et al. at col. 14, lines 21-24 does not disclose a password entered by the user at an "ordinary computer" and received by a remote authentication server at the time of the transaction as required by claim 1 as limited by claim 6. The password disclosed in Maes et al. is used for downloading a digital certificate and for accessing credit/debit card information encrypted and stored on a special PDA. Claim 6 is not anticipated by Maes et al.

Responding to paragraph 9 of the Office Action regarding claim 7, Maes et al. at col. 14, line 22, does not disclose a truncated CD with stored information read by an "ordinary computer" that is received by a remote authentication server for matching as required by claim 1 as limited by claim 7. There is no mention of a truncated CD in Maes et al. at all; the only smartcards disclosed are the magnetic stripe and embedded chip cards shown in Figs. 2(a) and 2(b) which are written by a special PDA in the main embodiment and read by a special ATM, kiosk or POS terminal in the alternative embodiment cited by the Examiner. Claim 7 is in no way anticipated by Maes et al.

Responding to paragraph 10 of the Office Action regarding claim 10, Maes et al. at col. 3, lines 17-37, does not does close a computer program module for insertion in a document generated on an "ordinary computer" information from storage media read by that "ordinary computer" which, along with a prompted-for personal code, is sent to an authentication server, as required by claim 10. Maes et al. does not mention documents at all, it discloses the receipt of credit/debit card information for encryption within a special PDA, the receipt of digital certificates by the special PDA and the decryption of the debit/credit card information and writing of the same by the special PDA. Maes et al. does not disclose copying of information

from the smartcard to the PDA, but from the PDA to the smartcard. Claim 10 is in no way anticipated by Maes et al.

Responding to paragraph 11 of the Office Action regarding claim 11, see the response to paragraph 3 above. Maes et al. does not disclose either of the first two steps of claim 11 that are performed by "any ordinary computer"; it discloses the use of a special PDA, ATM, kiosk or POS terminal. Maes et al. also does not disclose either of the second two steps of claim 11, the transmission of information from the storage medium and a personal code to an authentication server and the matching of that information to a data base of the authentication server based on the personal code. Maes et al. discloses transmission from a service provider of a digital certificate that is checked by the special PDA for validity. Claim 11 is not anticipated by Maes et al.

Responding to paragraph 12 of the Office Action, see the response to paragraphs 4 and 11 above. Maes et al. does not disclose any of the steps of reading information from a storage medium by "any ordinary computer" and transmitting that information through a second computer to the authentication server. Claim 12 is not anticipated by Maes et al.

Responding to paragraph 13 of the Office Action, see the response to paragraphs 5, 11 and 12 above. Maes et al. does not disclose any of the steps of reading information from a storage medium by "any ordinary computer" and transmitting that information and a personal code through a second computer to the authentication server. Claim 13 is not anticipated by Maes et al.

Responding to paragraph 14 of the Office Action, see the response to paragraphs 6 and 11 above. Maes et al. does not disclose any of the steps of reading a one-use token from a storage medium by "any ordinary computer" and transmitting that information through a second computer to the authentication server; Maes et al. does not even mention a one-use-token. Claim 14 is not anticipated by Maes et al.

Responding to paragraph 15 of the Office Action, see the response to paragraphs 7 and 11 above. Maes et al. does not disclose any of the steps of reading a digital certificate from a storage medium by "any ordinary computer" and transmitting that information through a second computer to the authentication server. Claim 15 is not anticipated by Maes et al.

Responding to paragraph 16 of the Office Action, see the response to paragraphs 8 and 11 above. Maes et al. does not disclose any of the steps of reading information from a storage medium by "any ordinary computer" and transmitting that information and a password through a second computer to the authentication server. Claim 16 is not anticipated by Maes et al.

Responding to paragraph 17 of the Office Action, see the response to paragraphs 9 and 11 above. Maes et al. does not disclose any of the steps of reading information from a truncated CD by "any ordinary computer" and transmitting that information through a second computer to the authentication server; Maes does not even mention a truncated CD. Claim 17 is not anticipated by Maes et al.

35 U.S.C. § 103(a) Rejections

Maes et al. in view of Lambert et al. does not make obvious claims 8, 9, 18, and 19. As discussed above in responses to paragraphs 3 and 11 of the Office Action, Maes et al. does not teach the system and process of base claims 1 and 11, but teaches away from them. Thus Lambert et al. cannot supply the limitations of claims 8 and 9, dependent from claim 1, and of claims 18 and 19, dependent from claim 2. This is clear from the fact that the objectives and approach of Maes et al. are different from that of Lambert et al. which would teach away from combining the two.

As reviewed above, Maes et al. is directed to the creation of a "Universal Card", in its primary embodiment, providing access, through the decryption of stored credit/debit card information if a previously downloaded digital certificate is valid and biometric data or a personal code is entered into the special PDA. An embodiment, cited by the Examiner, dispenses with the special PDA and migrates its functions to a special ATM, kiosk or POS

terminal. The credit/debit card information is then used in the normal course to conduct the underlying transaction. Lambert et al., in contrast, teaches a system of access to computer programs, applets, by generating keys from partial keys or tokens on a SmartCard (defined properly at col. 1, lines 40-43, but misused for magnetic stripe cards in Maes et al.) for decrypting such applets encrypted in one or more "stores" instead of identifying the user and looking up the user on an access list. Maes et al. teaches decryption the information on a storage medium for presentation to a transaction platform; Lambert et al. teaches decryption of information in a store available to the transaction platform.

Both Maes et al. and Lambert et al. require significant processing at different physical and logical locations as between the transaction parties, where the preferred mode is presentation of a storage medium at the point of contact with the transaction platform. In contrast, the instant invention is directed at the use of "any ordinary computer" capable of reading the medium and connected to a wide network, with the significant processing, being the real-time matching of information stored on the medium with information in a data base of a trusted third-party outside the transaction platform, which may or may not involve decryption. Maes et al.'s use of a service provider for providing a temporary digital certificate does not authenticate the transaction party at the time of the underlying transaction.

Responding to paragraphs 20 and 21 of the Office Action regarding claim 8, see the response to paragraph 3 above. Lambert et al. at col. 2, lines 2-13 and 30-33, together with Maes et al., do not disclose a wallet-sized storage medium with information uniquely associated with the transaction party and read by any ordinary computer, with a remote authentication server receiving that information along with a personal code, matching with its data base based on the personal code and authenticating the transaction party. The cited text from Lambert et al. calls for the use of partial encryption keys, which may or may not be unique to the transaction party, which, with the combination with a personal code at the transaction platform interface is used to generate a key for decryption of applets of a certain or lower level of security. Col. 1, lines 11-21 and 48-50 do not suggest the transmission from a storage medium at an ordinary computer to a remote authentication server of different stored information associated with different levels of

security; col. 1, lines 58-67, do not call for "lookup data" on a smartcard, but merely proposes that lookup tables used for access authorization after user identification is not as secured as the invention disclosed in Lambert et al. Nothing in Maes et al. or Lambert et al. suggests the transmission to and matching with a database at a remote authentication server of one of two groups of information uniquely associated with a transaction party read on an ordinary computer and the generation by the remote authentication server of an authentication for such a transaction. In particular, Lambert et al. does not perform authentication at all, but generates a generated from partial keys on storage media and a personal code to access a subgroup of applets. Accordingly, claim 8 is not obvious from Maes et al. in view of Lambert et al.

Responding to paragraph 22 of the Office Action regarding claim 9 see the responses to paragraphs 11, 20 and 21 above. Lambert et al. at col. 2, lines 2-13 and 30-33, together with Maes et al., do not disclose a wallet-sized storage medium with information uniquely associated with the transaction party and read by any ordinary computer, with a remote authentication server receiving that information along with a personal code, matching with its data base based on the personal code and authenticating the transaction party for one of at least two levels of transaction security or authority according to one of at least two corresponding personal codes of the transaction party. Lambert et al., in particular, discloses the use of only one personal code that is combined with partial keys to provide decryption keys. Accordingly, claim 9 is not obvious from Maes et al. in view of Lambert et al.

Responding to paragraph 22 of the Office Action regarding claim 18, see the responses to paragraphs 11, 20 and 21 above. Neither Maes et al. nor Lambert et al. nor the two together suggest the transmission of one of two stored tokens to a remote authentication server for matching with its database and authentication for a transaction of corresponding security or authority. . Accordingly, claim 18 is not obvious from Maes et al. in view of Lambert et al.

Responding to paragraph 23 of the Office Action regarding claim 18, see the responses to paragraphs 11, 20 and 21 above. Neither Maes et al. nor Lambert et al. nor the two together suggest the transmission of one of two stored tokens to a remote authentication server for

matching with its database and authentication for a transaction of corresponding security or authority. Accordingly, claim 18 is not obvious from Maes et al. in view of Lambert et al.

Responding to paragraph 24 of the Office Action regarding claim 19, see the responses to paragraphs 11, and 20-22 above. Neither Maes et al. nor Lambert et al. nor the two together suggest the transmission of a stored token and one of two personal codes to a remote authentication server for matching with its database and authentication for a transaction of corresponding security or authority. Accordingly, claim 19 is not obvious from Maes et al. in view of Lambert et al.

Rejection Under the Doctrine of Obviousness-Type Double Patenting

Claims 1-3 and 11 are provisionally rejected under the doctrine of obviousness-type double patenting as being unpatentable over claims 1-3, and 9 of copending Application No. 10/132438. This rejection is provisional because the conflicting claims have not in fact been patented.

Applicants respectfully submit that the response to the provisional rejection must also be provisional as claims 1-3 and 11 are herein amended and they have not yet received an Office Action on claims 1-3 and 9 of the copending application, amendment of which may obviate any obviousness-type double patenting. As the copending application claims the priority dated of this application, it would appear that if patents issued on both applications, they would expire on the same date, making unnecessary any terminal disclaimer. Only if there were a patent term extension longer in one of the two patents issuing on these applications would there be a necessity to have a terminal disclaimer. The instant application, by the same inventors and assigned in whole to the same entity as the copending continuation-in-part application which claims priority of this application, would appear to have priority. If it issues first, and is in a form that still subjects the later application to an obviousness-type double patenting, it may be appropriate to disclaim any additional term of the later application as well as its enforceability if common ownership ceases. If the later application issues first in a form that subjects this

application to an obviousness-type double patenting, it may then be appropriate to disclaim any additional term of this application as well as enforceability if common ownership ceases. Accordingly, following is a provisional terminal disclaimer for the second contingency:

The term of the patent issuing from Application No. 09/816975 shall end at the end of the term of the patent issuing from Application No. 10/132438.

The assignee owns the entire interest in this Application.

Any patent granted on this Application shall be enforceable only for and during such period that said patent is commonly owned with a patent earlier issuing from Application No. 10/132438.

Conclusion

For the reasons set forth above, Applicants believe the application is in condition for allowance. Applicants thus request that the Examiner withdraw the rejections and grant favorable consideration and allowance. Upon review of this paper, the Examiner is invited to contact the undersigned at 617-854-4000.

Respectfully submitted,

Jayme Matthew FISHMAN et al.,
Applicants

Dated: June 8, 2004

By: _____

Stephen Y. Chow
Reg. No. 31,338
Attorney for Applicants

13230-101OAResp